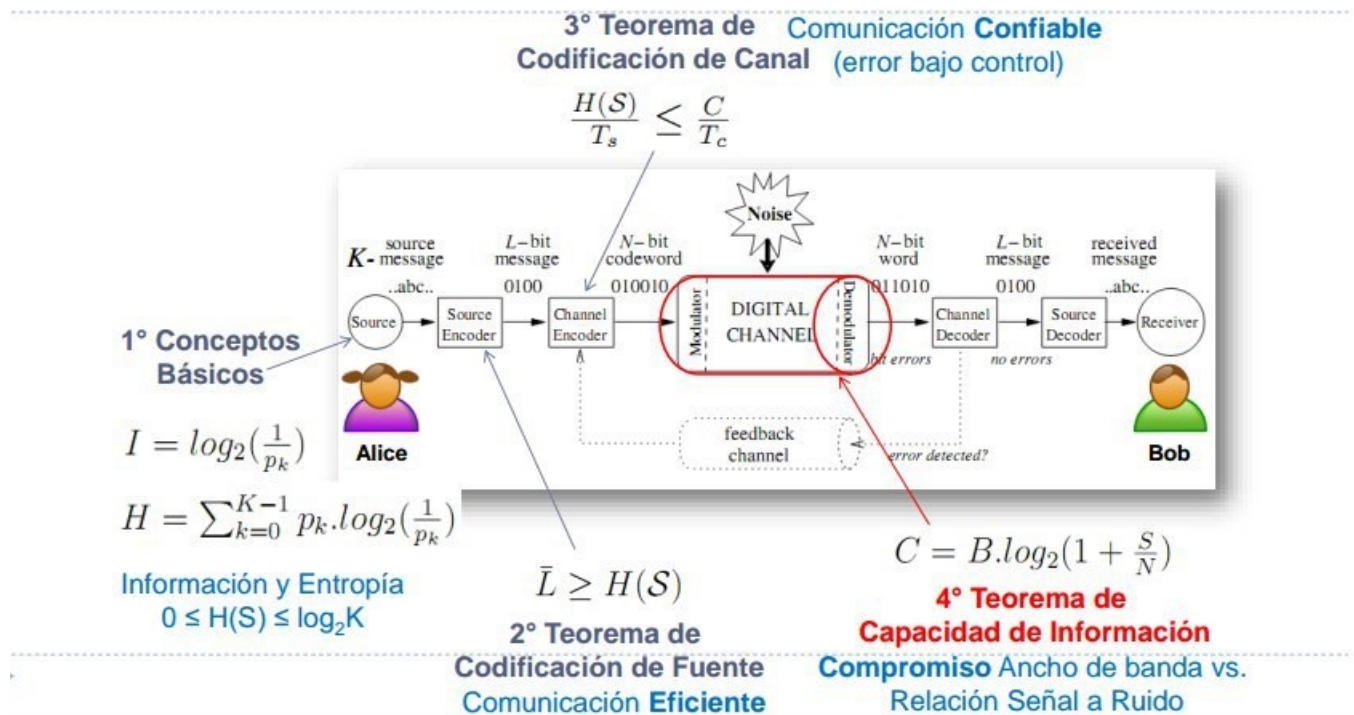


1. Explique mediante Teoría de la Información la relación entre una fuente de datos aleatoria de memoria nula y la posibilidad de Transmitir los símbolos generados en un canal binario sometido a ruido.

## Marco de Referencia



En telecomunicaciones, codificamos las ondas senoidales con 0s y 1s. Estas señales son enviadas por un canal: cuando la señal es alta, se codifica como un 1, y cuando es baja, con un 0. Llamamos eventos de información a estos 1s y 0s.

Shannon argumentó que la radio, la televisión o el teléfono podían ser pensadas de la misma manera y que todos los mensajes, independientemente del canal, estaban potencialmente en riesgo de una entrega incorrecta debido al ruido. Él propuso que un mensaje debía ser concebido como una secuencia con propiedades estadísticas, las cuales se podrían entender, estudiar y codificar para permitir una transmisión efectiva, es decir, que use la menor cantidad de recursos del canal para transmitir el

mensaje (eliminar redundancia). Cuanto mayor es la entropía del mensaje, más esfuerzo se necesita para transmitirlo. Entonces, estableció la Teoría Clásica de la Información, que se basa en dos teoremas fundamentales:

1. Codificación para una fuente sin ruido.
2. Codificación para un canal ruidoso.

Sea  $E$  un suceso que puede presentarse con probabilidad  $P(E)$ . Cuando  $E$  tiene lugar decimos que hemos recibido  $l(E) = \log 2P(E)$  bits. Si la probabilidad es 0, la información es infinita. Si la probabilidad es 1, la información es 0.

Una fuente de memoria nula es una fuente que emite una secuencia de símbolos pertenecientes a un alfabeto finito y fijo, por ejemplo,  $S = \{1, 0\}$ . La probabilidad de observar el próximo símbolo es independiente de los símbolos emitidos anteriormente. Entonces, podemos calcular la información que aporta cada símbolo a la fuente:  $l(s_i) = \log(p(s_i))$ . Luego, también podemos calcular la cantidad media de información por símbolo de una fuente, conocida como entropía de la fuente, de la siguiente manera:

$$H(S) = \sum_{S_i \in S} P(S_i) \cdot I(S_i)$$

La entropía es máxima cuando todos los valores posibles de la variable  $s$  son equiprobables.

Nos interesa saber cómo podemos transformar esos símbolos que nos vienen en secuencias de bits (códigos), que sean lo más eficiente posible, es decir, que utilicen la menor cantidad de bits posibles, eliminando redundancia. Normalmente, una codificación debe ser de bloque, singular y separable (unívocamente de-codificable). Para que un código sea eficiente, vamos a tener que asignar palabras de código más cortas a los

símbolos de la fuente más probables, porque al ser los más probables, es esperable que sean los que más aparecen en los mensajes. Notación:

- $l_i$ : longitud de la palabra que codifica al símbolo  $s_i$  de la fuente.
- $p_i$ : probabilidad de aparición de  $s_i$ .
- $r$ : cantidad de símbolos diferentes del alfabeto del código.
- $L = \sum_i p_i l_i$ : longitud media de un código:

Notemos que para que un código sea eficiente, se debe cumplir que la longitud media del mismo, sea mayor o igual a la entropía de la fuente, es decir:

$$L \geq H(S)$$

La condición necesaria y suficiente para que un código sea **instantáneo** es que sus palabras cumplan con la condición de los prefijos, es decir, que no exista palabra que sea prefijo de otra palabra de longitud mayor. La idea es que el receptor sea capaz de, una vez detectado un símbolo, no tenga que esperar a los siguientes bits para verificar si en realidad se trataba de un prefijo de otra palabra de longitud mayor.

La condición necesaria y suficiente para la existencia de un código instantáneo de longitudes es que

$$\sum_{i=1}^q r^{(-l_i)} \leq 1$$

conocida como inecuación de Kraft, donde  $r$  es la cantidad de símbolos de la fuente.

La distancia entre el emisor y el receptor, el ruido, la temperatura del medio, Diafonía, etc. producen perturbaciones en el canal. Estas hacen que el receptor tenga que deducir la señal original a partir de la señal recibida con ruido, pudiendo cometer errores (cuando tenía que leer un 1, leí un 0). A la tasa de errores por segundo, la llamamos BER (Bit Error

Rate).

Notación:

C: Velocidad de transmisión de datos, en bits por segundo.

B: Ancho de Banda, en Hz.

N: nivel medio o potencia de ruido a través del canal.

S: Potencia de la señal. Lo podemos pensar como la Amplitud.

SNR: Relación Señal-a-Ruido.

Para un cierto N, a mayor C, mejoramos en cuanto a que tenemos un menor período de un bit, pero empeoramos en cuanto a que tenemos una mayor tasa de error. En base a esto, Shannon identificó que era importante estudiar esta relación entre la potencia de la señal y la potencia del ruido SNR (Relación Señal-a-Ruido). En principio, si se aumenta el ancho de banda B y la potencia de la señal S, aumenta la velocidad de transmisión C. Pero, al aumentar el ancho de banda B, aumenta el ruido, porque le estamos abriendo las puertas a más frecuencias con más ruido (no es lineal). Además, si aumentamos la potencia de la señal, aumenta las no linealidades, y por tanto el ruido de Intermodulación. En base a estas observaciones, Shannon define la velocidad de transmisión teórica máxima como:

$$C_{max} = B \cdot \log_2(1 + SNR)$$

Entonces, tenemos que la velocidad de transmisión depende del ancho de banda, que a su vez depende de las características físicas del canal, y la relación SNR, donde el ruido depende del canal, mientras que la potencia de la señal depende de la señal transmitida. Y por ultimo, para describir todas las ecuaciones del diagrama, la formula:

$$H(S)/T_s \leq C/T_c$$

Hace referencia al límite absoluto de la tasa de transmisión utilizada para transportar una señal de manera confiable a través de un canal ruidoso o límite de la confiabilidad:

Teorema de codificación de Canal (comunicación confiable) Nos indica una relación entre la entropía, la tasa con la que emitimos símbolos de la fuente, y la tasa con la que emitimos códigos de un channel encoder. Esta inecuación en conjunto con la capacidad máxima de un canal, brindadas por Shannon y basada en la ley de los grandes números, nos dice que mientras mientras mantengamos el rate de envío de mensajes por un canal más bajo que la capacidad del canal, entonces existe un channel encoder-decoder que nos permiten una comunicación sin error virtualmente (un error tan chico como se quiera).

2. Explicar la relación que existe entre Delay y RTT. Enumerar los componentes del Delay en una conexión, especificando cuáles son en general despreciables y cuáles son en general significativas. Dar un ejemplo de una comunicación entre un nodo emisor y un nodo receptor con Delays asimétricos (o sea, un caso en el que predomine un tipo de delay en particular y otro caso en el que predomine otro distinto). Realice un diagrama de una topología genérica de red ubicando donde ocurren cada uno de ellos.

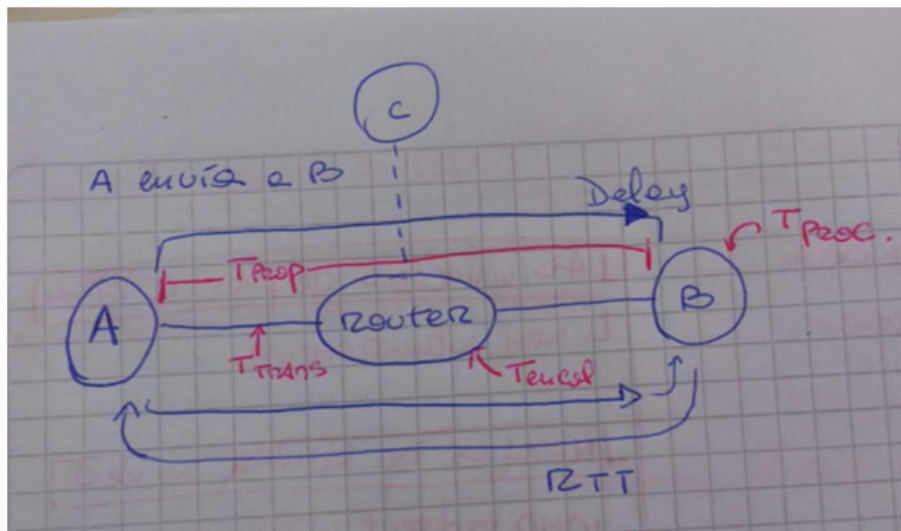
El Delay es el tiempo que tarda un mensaje en llegar de un extremo al otro. El RTT (Round-Trip Time) es el tiempo que se tarda entre que se envía un mensaje y se recibe el correspondiente ACK. Entonces, en un principio, se podría pensar que  $RTT = 2 * Delay$ , pero este está conformado a su vez por distintos tiempos que pueden variar entre la ida y la vuelta. Desglosado el Delay se conforma por:

$$Delay = T_{prop} + T_{trans} + T_{encol} + T_{proc}$$

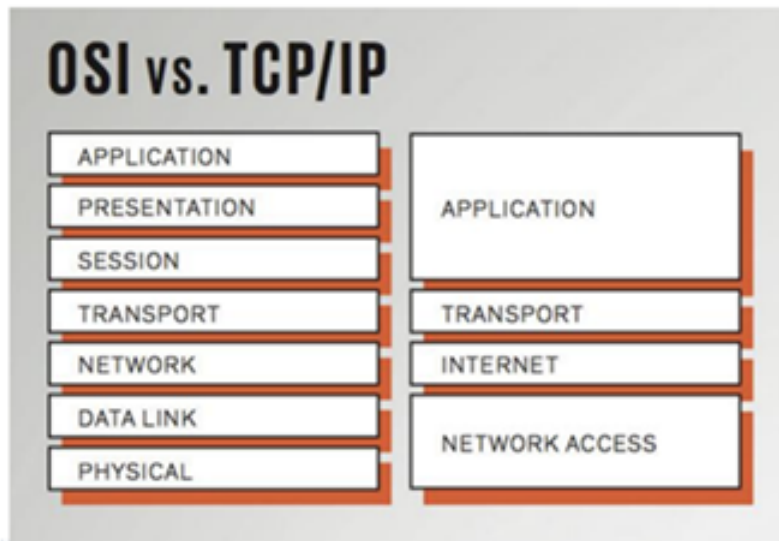
Donde tenemos que:  $T_{prop}$  = Tiempo de propagación. Una vez que el bit es “empujado” en el medio, el tiempo que tarda en llegar al otro extremo. La velocidad de propagación depende más que nada de la distancia en el medio físico. Generalmente es cercana a la velocidad de la luz.  $T_{trans}$  = Tiempo de transmisión. Es el tiempo requerido para “empu-

jar” todos los bits de un paquete en el medio de transmisión.  $T_{\text{encol}}$  = Tiempo de encolamiento (Retardo de colas). Tiempo que el paquete espera en un buffer hasta ser transmitido. Este tiempo depende del tamaño de las colas y el nivel de congestión de la red.  $T_{\text{proc}}$  = Tiempo de procesamiento. Decisión de ruteo de paquetes, también puede incluir chequeo de errores.

Generalmente se desestiman los últimos dos tiempos. Puede suceder en una comunicación entre emisor y receptor, que a la hora de contestar algún mensaje el tiempo de encolamiento aumente considerablemente debido a la congestión en la red. También, por falla en algún nodo intermedio, el tiempo de propagación puede verse afectado. Por eso se puede llegar a producir diferencias en el tiempo de ida y vuelta en una comunicación.



3. Enumere y describa brevemente las capas del Modelo TCP/IP de comunicaciones. Mencione al menos una tecnología o protocolo asociado a cada capa. Compare conceptualmente el modelo TCP/IP con el modelo OSI propuesto para los mismos objetivos.



El modelo TCP/IP está definido por las siguientes 4 capas:

1. La capa de acceso a internet, se encarga de la transmisión de bits sobre los canales de comunicación y de la manipulación de frames. Emplea las tecnologías como MACs para realizar el circuito virtual y Switchs, como hardware. 1. Física cables y Ethernet. 2. Switchs y MAC para capa 2 de OSI.

2. La capa de internet realiza el ruteo de paquetes en la red switchheada, mediante direcciones IPs y protocolo IP, como tecnología de software y Routers, como hardware.

3. La capa transporte se encarga de la comunicación interproceso (mensajes), mediante los protocolos TCP y UDP. El primero orientado a la conexión y a la seguridad del paquete, el segundo a la no conexión y a la velocidad.

4. La capa de Aplicación es donde se da significado a los datos que se envían. Se basa principalmente en tecnologías de software, http, smtp, Dns.

Aplicación	Web (HTTP)	Transf. arch. (FTP)	e-mail (SMTP)	Resol. nombres (DNS)	Vídeo streaming	Telefonía
Transporte	TCP (Transmission Control Prot.)			UDP (User Datagram Prot.)		
Red	IP (Internet Protocol)					
Enlace	Ethernet	WiFi		ADSL		CATV
Física	Cable o Fibra	Radio		Cable telefónico		Cable coaxial

4. Explique la diferencia entre los protocolos de acceso múltiple CSMA/CD y CSMA/CA y muestre dos tecnologías que los implementan.
- ¿A qué capa del modelo TCP/IP pertenecen?
  - ¿Cómo podría un dispositivo interconectar dos nodos que usan uno y otro mecanismo?

Los protocolos son Carrier Sense Multiple Access y difieren en si son Collision Detection o Collision Avoidance. Ambos protocolos determinan cómo acceden distintos hosts al medio compartido y qué deben hacer para evitar o solucionar un problema de colisión.

### **Collision Detection:**

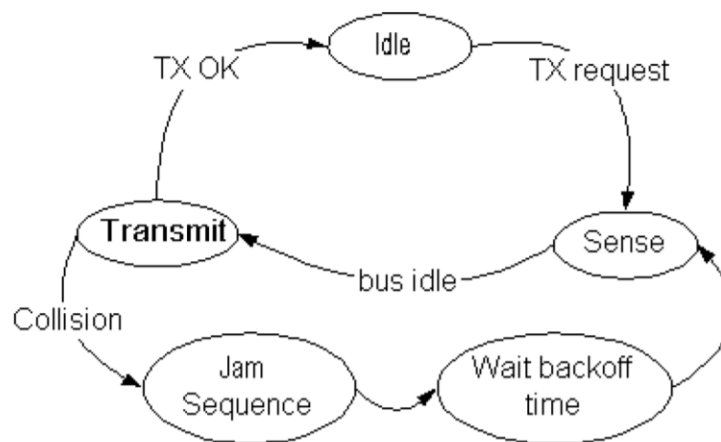
- Cuando un host tiene datos para enviar, sensa el medio
- Si está libre transmite
- Si está ocupado, espera a que se libere y transmite con probabilidad  $p$  (Algoritmo  $p$ -persistente).
- Al enviar se continúa sensando el medio mientras se transmite. Si se detecta una colisión, se inserta una Jam Sequence (Señal que reafirma la interferencia) se debe retransmitir:
- Se utiliza Exponential Backoff para determinar cuánto esperar hasta la retransmisión.
  - Elegir un número al azar  $z$  entre 0 y  $2*(k-1)$  con  $k$  la cantidad de reintentos.



- Esperar  $z$  veces el máximo RTT de la red antes de sensar para retransmitir.
- Este protocolo se utiliza para redes half-duplex. Hoy en día queda como retrocompatibilidad.
- Ethernet usa CSMA/CD y es 1-persistente. La longitud mínima de un frame es 64 bytes. Un host sólo puede detectar una colisión mientras está transmitiendo una señal. Por lo tanto, debe permanecer suficiente tiempo para asegurarse de que ningún otro host ha comenzado a transmitir en el interín. En otras palabras, debe tener suficiente cantidad de datos para transmitir.

## Estados de un Transmisor CSMA-CD

---



### Collision Avoidance:

- En Wireless se utiliza este protocolo porque no se puede sensar el medio para determinar si hay colisión. Esto se debe a que la potencia de la señal emitida es mucho más grande que la recibida.
- Antes de transmitir, una estación determina el estado del medio.
- Si el medio está libre, espera un tiempo denominado DIFS (DCF Inter-frame Space) y luego transmite. Al finalizar la transferencia, el receptor espera un tiempo SIFS y luego transmite un ACK en caso de que haya

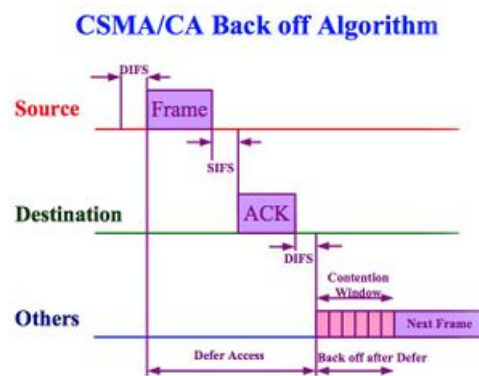
recibido todos los datos exitosamente. Si no se transmite el ACK, el emisor ejecuta el algoritmo de Exponential Backoff:

- Se establece una contention window (ventana de slots de tiempo, análoga al backoff de CSMA/CD).

- Se elige un backoff counter al azar, que determina la cantidad de slots de la ventana durante los que vamos a esperar.

- Mientras el canal esté libre, se decrementa el backoff counter (en caso contrario se mantiene). Cuando el backoff counter llega a 0, se intenta transmitir el frame (comienza CSMA/CA de nuevo).

- Si la transacción no es exitosa, se selecciona una contention window del doble de tamaño de la anterior.



### Problemas que resuelve CSMA/CA (vs CSMA/CD):

Nodos ocultos: Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo al que no escucha.

Nodos expuestos: Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que escucha no le interferiría.

Esto se produce a nivel de capa de enlace, y los nodos se conectan por switches.

CSMA/CD fue usado en las -ahora obsoletas- variantes de Ethernet 10BASE5 y 10BASE2. Actualmente las modernas redes Ethernet construidas con switches y conexiones full-duplex lo mantienen como modo

de retrocompatibilidad.

5.Explique por qué se considera que mecanismo de control de Congestión de TCP tiene un comportamiento “equitativo” (por ejemplo tengo varias aplicaciones que usan TCP desde distintos dispositivos en mi casa accediendo a Internet , usando todos el mismo router, “acceso de banda ancha” ) cuando diversos flujos comparten el mismo recurso.

Aunque ambos se basan en switcheo de paquetes y datagramas (no circuitos virtuales) con control de errores, TCP mantiene un servicio orientado a conexión con confiabilidad, control de congestión y flujo, mientras UDP envía con una política best-effort sin preocuparse siquiera que el receptor sea alcanzable o esté disponible, ni el estado de la red por la cual el paquete debe viajar.

El emisor en TCP tiene protocolos para intentar no dejar recursos ociosos como también rápidamente salir de la congestión reduciendo a la mitad la ventana de emisión efectiva en casos de RTO. Estas cosas se efectúan con las adaptaciones sobre Sliding Window como fast recovery, fast retransfer, slow start, técnicas para cálculo de RTT y RTO, etc. Por otro lado, la aplicación que utilice UDP tendrá que ser responsable sobre los paquetes que no lleguen a destino e implementar políticas al respecto, ya que UDP no le provee nada. Por estas razones, hay firewalls que bloquearon históricamente implementaciones basadas en UDP:

**Additive Increase / Multiplicative Decrease:** (mínimo entre congestion window y advertised window). CW se reduce cuando se detecta una suba en la congestión, y se aumenta cuando baja. Cada vez que ocurre un timeout, se baja CongestionWindow a la mitad (con un mínimo en el MSS). Cada vez que llega un ACK, la ventana se incrementa por una fracción del MSS)

**Slow Start:** El comportamiento de AIMD sirve cuando se está operando cerca de los límites permitidos por la red, pero es muy conservador arran-

car todas las conexiones transmitiendo con ventana mínima y subiendo linealmente. Slow Start hace este incremento exponencial. Además de en el inicio de la conexión, el mecanismo se utiliza cuando se comienza a enviar de nuevo tras la pérdida de paquetes.

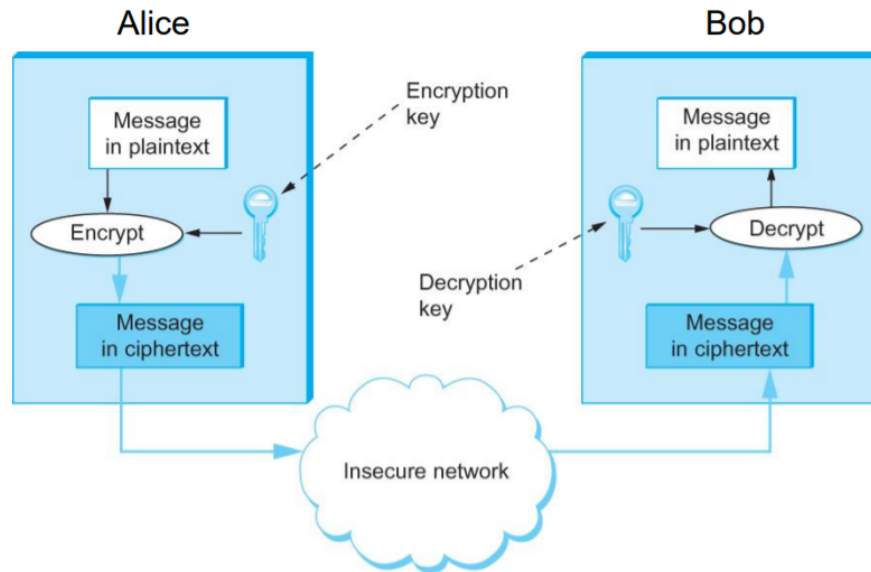
**Fast Retransmit - Fast Recovery:** Se implementa haciendo que el receptor envíe un ACK por cada paquete que llega (aunque sea fuera de orden y tenga que mandar un ACK duplicado de un paquete anterior. Cuando el emisor detecta cierta cantidad de ACK duplicados, retransmite el segmento con número siguiente al ACK (sin necesidad de esperar el timeout).)

**El TCP Reno** continuó usando las mejoras incorporadas en el TCP Tahoe, así mismo modificó la retransmisión rápida para adicionar el Fast Recovery (recuperación rápida). Esta nueva implementación previene que se vacíe el caño (“pipe”) después de la retransmisión rápida, por lo que evita la necesidad de llenarlo con el algoritmo Slow-Start luego de haber sufrido la pérdida de un solo paquete.

6. Realice 2 esquemas que pongan en evidencia la diferencia entre el sistema de criptografía de Clave Simétrica y el sistema de criptografía de Clave Pública, para una comunicación entre dos usuarios diferentes A y B que requieren enviar información confidencial a un tercer usuario C por medio de una red insegura. Describa una ventaja y una desventaja de cada método.

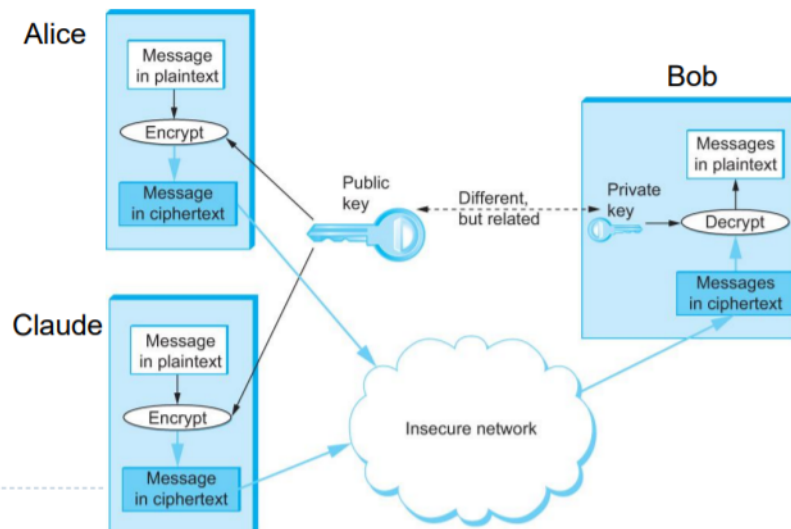
6.b.Explique la diferencia entre los conceptos de confidencialidad, integridad, autenticación y no repudio en el contexto de seguridad informática.

# Criptografía Simétrica



## Criptografía de clave pública

- ▶ Las claves de encriptado (**pública**) y desencriptado (**privada**) son lo suficientemente diferentes como para que la segunda no pueda calcularse a partir de la primera.



▶ 33

El esquema de clave pública y clave privada deviene de técnicas de

criptografía asimétrica: Se utilizan claves distintas para encriptar y desencriptar los datos. En particular el esquema de clave pública y privada consiste en: Se tiene una clave pública que todo el mundo podría ver, y una privada que no debería ser expuesta. No se puede inferir una clave a partir de la otra. Se utiliza generalmente el método RSA: A partir de propiedades matemáticas respecto de los números primos se pueden derivar pares de claves.

Para la Capa de Red, IPsec es el protocolo que, a nivel de datagrama se agrega:

- Authentication Header (AH) proporciona integridad, autenticación y no repudio.
- Encapsulating Security Payload (ESP) proporciona confidencialidad.

**Confidencialidad:** Los mensajes sólo deben poder ser entendidos por las partes especificadas en la comunicación.

**Integridad:** Los mensajes enviados no pueden ser modificados durante su transmisión.

**Originalidad:** El mensaje no es una copia artificial repetida.

**Temporalidad:** El mensaje no fue demorado maliciosamente.

**Autenticación:** Ninguna parte puede asumir en forma no autorizada la identidad de otra parte.

Control de acceso (Autorización): Solo ciertos usuarios remotos pueden realizar ciertas acciones permitidas (ataque DNS).

**Disponibilidad:** Todo usuario potencial tendrá su oportunidad de ser considerado y eventualmente admitido (ataque DoS).

**No Repudiación:** Ninguna de las partes puede negar haber participado en una transacción.

Ventajas:

Emisor y receptor no comparten una clave secreta. En este sentido escala mejor que la criptografía simétrica (un mismo mensaje encriptado con la privada puede ser leído por todos los que conocen la clave pública).

Se puede compartir la clave pública para recibir mensajes encriptados de distintas fuentes.

Desventajas:

Es computacionalmente más caro que la encriptación simétrica.

Es difícil verificar de quien es una clave publica.

El largo de las claves suele ser mayor.

7.Explique la diferencia entre dominio de broadcast y dominio de colisión en una LAN y cómo se puede usar direccionamiento IP para conectar distintas LAN. Cómo se separan. Qué es una VLAN. Cómo funciona en capa 2 (enlace) y en capa 3 (red).

Cuando un equipo quiere enviar un paquete a toda la red (LAN), el dominio de broadcast define quienes lo reciben. Por otro lado, en cada tramo del envío de un paquete, este puede colisionar con otros paquetes que viajan por el mismo medio físico. Los equipos con los cuales puede colisionar en un determinado tramo, es el dominio de colisión (de ese tramo).

Tanto MAC como IP buscan identificar unívocamente un nodo en la red. A diferencia de las direcciones MAC, dos hosts en una misma LAN comparten información en sus IPs que nos brindan una noción sobre su ubicación. Una forma de extender redes LAN con IP es asignando IPs privadas con una misma subnet a los equipos de una red pequeña (LAN) y una IP privada a cada router de esa LAN. Cada router tendrá una tabla de traducción NAT para mapear <IP publicas, puerto> (si es que hay) a <IPs privadas, puerto> al momento en que nodos de una LAN quieran comunicarse con otra. Para extender las LAN, interconectándolas con otras, las IPs públicas de routers cercanos van a compartir también una misma máscara. Cada grupo de LANs define un área, y para cada una definimos un router frontera que condensa toda la información de ruteo interno, y así restringir a su vez los dominios de algoritmos de

ruteo interno. El dominio de colisión, tanto como el de broadcast queda restringido a la red hogareña. Ahora los routers de un área no conocen los routers fuera de ella, y los routers frontera se comunican entre ellos a través de routers troncales, entre los cuales se utilizan otros algoritmos de ruteo interno. Esto último forma un sistema autónomo (red del ISP), el cual se interconecta con otros AS a través de uno o mas routers fronteras del AS. Los routers frontera de AS son lo que un router frontera de area local para un ISP(Internet Service Provider).

**Una VLAN**, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en una única red física. Son útiles para reducir el dominio de broadcast y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa OSI 3 y 4). Son implementadas por switches en capa 2. Aunque las más habituales son las VLAN basadas en puertos (nivel 1), las redes de área local virtuales se pueden clasificar en cuatro tipos según el nivel de la jerarquía OSI en el que operen:

**VLAN de nivel 1 (por puerto).** También conocida como “port switching”. Se especifica qué puertos del switch pertenecen a la VLAN, los miembros de dicha VLAN son los que se conecten a esos puertos. No permite la movilidad de los usuarios, habría que reconfigurar las VLAN si el usuario se mueve físicamente. Es la más común.

**VLAN de nivel 2 por direcciones MAC.** Se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se conecta a otro puerto de ese u otro dispositivo. El principal inconveniente es que hay que asignar los miembros uno a uno y si hay muchos usuarios puede ser agotador.

**VLAN de nivel 3 por tipo de protocolo.** La VLAN queda deter-



minada por el contenido del campo tipo de protocolo de la trama MAC. Por ejemplo, se asociaría VLAN 1 al protocolo IPv4, VLAN 2 al protocolo IPv6, VLAN 3 a AppleTalk, VLAN 4 a IPX...

**VLAN de nivel 4 por direcciones de subred (subred virtual).** La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece. En este tipo de VLAN son los paquetes, y no las estaciones, quienes pertenecen a la VLAN. Estaciones con múltiples protocolos de red (nivel 3) estarán en múltiples VLAN.

**VLAN de niveles superiores.** Se crea una VLAN para cada aplicación: FTP, flujos multimedia, correo electrónico, etc. La pertenencia a una VLAN puede basarse en una combinación de factores como puertos, direcciones MAC, subred, hora del día, forma de acceso, condiciones de seguridad del equipo, etc.

#### 8. Diferencias entre RIP y OSPF.

- a. En los algoritmos de ruteo link-state y en especial OSPF se dice que se realiza una "inundación confiable". ¿Podría explicar este concepto? .
- b. En los algoritmos de ruteo link-state, en especial el protocolo OSPF, se dice que se realiza un cálculo centralizado. Explique a qué se refiere.
- c. En los algoritmos de ruteo distance-vector, en especial el protocolo RIP, se dice que realiza un cálculo distribuido. Explique a qué se refiere.

- **Implementaciones:** RIP está basado en Distance Vector, mientras OSPF en Link State.

- **Memoria/recursos en nodos:** RIP guarda un vector que indica para cada nodo, a qué distancia está (en RIP se usan hops del camino) y cual es el siguiente HOP al que hay que ir para realizar el camino mínimo (guardamos uno solo). En OSPF, cada nodo tiene potencialmente todo el grafo, que ocurre cuando tiene los paquetes LSP de todos, y es capaz de computar los caminos mínimos de todos a todos (lo cual es útil si queremos distribuir los paquetes por distintos caminos). Lo que hace que OSPF utilice más recursos en cada nodo.

- **Comunicación:** Distance Vector envía toda la información que sabe solamente a sus vecinos, mientras que OSPF realiza una inundación “confiable” sólo con lo que sabe de su relación con sus vecinos. Decimos que es confiable porque los paquetes vienen con un TTL que se descuenta en cada hop y al llegar a 0 se descartan de la red, con un número de secuencia que permite a cada nodo comparar y descartar si la información ya la conoce, autenticación y ACKs entre nodos. Estas decisiones nos aseguran que la inundación sea “controlada” y converja más rápido que RIP. Por otro lado RIP sufre un problema, llamado conteo infinito y para evitarlo, implementa varias heurísticas, como un límite máximo en la distancia en los caminos (fijo en 16), si nodo A le va a enviar su información a su vecino B y tiene caminos de la pinta  $A -> B -> \dots -> Z$ , entonces a B le informa que llega con distancia infinito a Z, y así evitar que B piense que puede llegar a Z a través de A (split horizon with poison reversed).
- **Actualización de información:** En RIP se actualiza la información si el nuevo camino es más corto que el existente y los nodos periódicamente comparten esta información. En OSPF, un nodo A tiene la información de todos los otros LDPs de otros nodos que llegaron con su TTL hasta él, con el último SEQ Number que le llegó, descarta cada cierto tiempo la información y hace un pedido nuevo de información a estos nodos.
- **Algoritmo:** RIP ejecuta un algoritmo basado en bellman ford distribuido entre todos los nodos. OSPF ejecuta un Dijkstra modificado en cada uno de los nodos, cada uno con su grafo, mientras va recibiendo información. Por lo que OSPF es más complejo, y realiza más operaciones, pero en la práctica converge más rápido.
- **En que momentos corre:** RIP envía periódicamente estos paquetes a la red. OSPF a demanda.

### **Problema de Conteo infinito de RIP:**

Ocurre cuando un grupo de nodos se informan mutuamente que pueden llegar a un tercero yendo uno a través del otro, cuando en realidad no

es así. Por ejemplo, si tenemos una red con la pinta A-B-C y A se cae, B marca que ahora llega a A con distancia infinito, pero antes de comunicárselo a C, C le envía a B que llega con distancia 2 a A, entonces B actualiza su camino A con distancia  $2+1$  y se lo envía a C. C hacia su camino a través de B, entonces actualiza su camino a A en  $3+1$ , y así sucesivamente.

9. Explicar Random Early Detection, y ubicar su implementación en un diagrama de topología de red simple de lazo cerrado (o sea closed loop) de TCP (aclaración: "ubicar la implementación" quiere decir dibujar un par de compus y routers, y decir en cuáles se ejecuta RED y en cuáles no, y muy sintéticamente qué se ejecuta en los nodos en los que no se ejecuta RED).

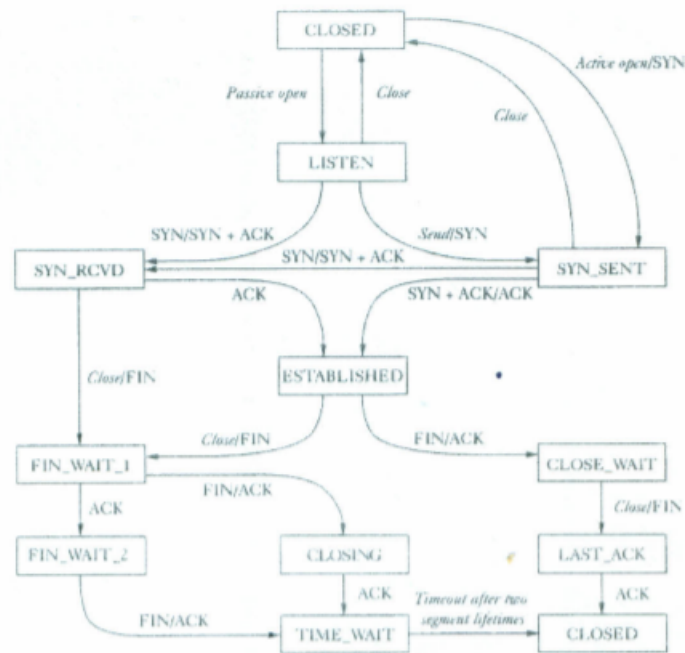
RED es un protocolo para controlar la congestión de una red, de tipo lazo cerrado e implícito porque la red descarta paquetes al aproximarse a la congestión y el emisor infiere congestión de forma implícita al tener timeout en sus paquetes, ACKs duplicados, etc.

Los routers miden la saturación de sus buffers, y en base a estos deciden si dropear o no los paquetes que entran. Más en detalle, cada uno tiene dos thresholds  $MIN\_T$  y  $MAX\_T$ , y una probabilidad máxima  $P$ . Van a ir sensando la saturación de sus buffers. Si la saturación  $< MIN\_T$ , entonces rechazan los paquetes con probabilidad 0. Si  $MIN\_T \leq \text{saturación} < MAX\_T$ , entonces los paquetes nuevos se rechazan con probabilidad  $P * (\text{saturación} - MIN\_T) / (MAX\_T - MIN\_T)$ . Si  $MAX\_T < \text{saturación}$ , los paquetes entrantes se rechazan con probabilidad 1. Generalmente se quiere que los cambios de saturación en el tiempo sean suaves para no ser tan sensibles a picos de cambios, por lo que se actualiza utilizando técnicas como con RTO. Es decir, una actualización convexa en base a nueva y vieja información, utilizando desvíos.

El emisor, que está comunicándose a través de TCP, asume congestión cuando se pierde el paquete por el RTO, y reduce su ventana de trans-

misión.

10. Describa los procesos de establecimiento y cierre de una conexión TCP. En la liberación de una conexión TCP, ¿Cómo se “resuelve el problema de los dos ejércitos”?

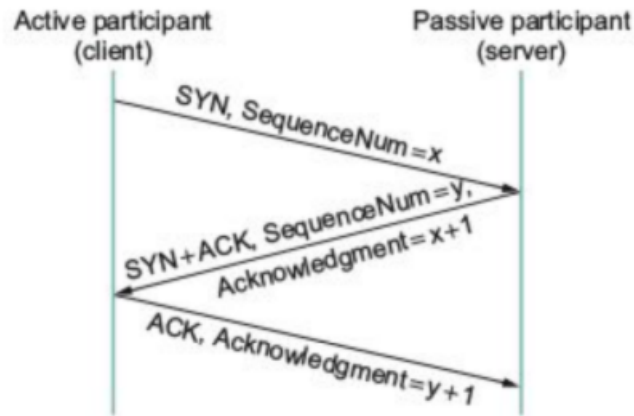


En TCP el establecimiento de conexión sucede generalmente por el protocolo 3-way handshake. Supongamos un inicio de conexión entre los hosts A y B:

A envía un paquete con flag SYN, indicando que quiere abrir una conexión.

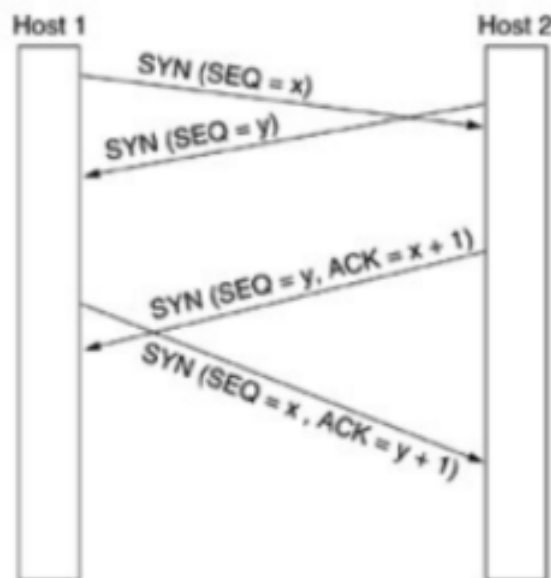
B reconoce el SYN, y le confirma con un ACK + SYN

A reconoce el SYN con un ACK.



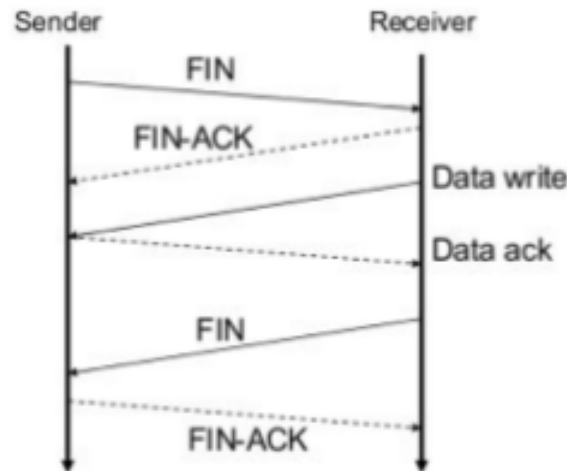
Observaciones: Los SYN se secuencian y cuentan como 1 byte. Esto es porque solo se hace ACK de cosas secuenciadas y queremos reconocerlos. Los Sequence Number iniciales son un número al azar con la finalidad de evitar reencarnaciones de segmentos de conexiones anteriores.

Puede suceder también, aunque no es usual, que ambos hosts quieran comenzar la conexión en simultáneo. Este caso también está contemplado por el protocolo TCP:



Notar que el segundo SYN que se mandan es para reafirmar el SYN

inicial (Tiene el mismo número de secuencia).



En cuanto al cierre de conexión el caso más típico es el four-way handshake:

A envía un paquete con flag FIN indicando que no enviará más datos.

B reconoce el FIN con un ACK. Puede seguir enviando datos.

B envía un paquete con flag FIN para indicar su cierre de conexión.

A reconoce el FIN enviando un ACK.

Si se pierden segmentos FIN, hay timers que intentarán reenviar una determinada cantidad de veces, hasta dar por terminada la conexión. Si se pierden ACKs no reintentan. Cuando se vence timers cierran.

11.Explique sintéticamente la organización del espacio de nombres en DNS y describa sus dos tipos principales de mecanismos de consulta.Diferencia entre consulta recursiva e iterativa. Cuándo suceden?

La diferencia está en que en la iterativa si el local DNS server no tiene la respuesta le irá preguntando a servidores autoritativos la información de distintas jerarquías e ira resolviendo la dirección IP final. En recursiva, cada servidor DNS se ocupa de resolver un dominio en particular. En ambas los DNS server podrán ir cacheando las respuestas.

## Revision

Tu equipo tiene configurados DNS Servers, y hace queries recursivas porque no sabe resolver de manera iterativa la ip de un dominio. Las queries recursivas regresan con la respuesta o error.

Todos los DNS Servers son iterativos. Supongamos queremos resolver `www.example.com` .

Si el DNS Server tiene la respuesta cacheada, la devuelve.

Si no la tiene, va a queriar a su Root DNS Server para saber a quien preguntarle por el dominio `.com`. La respuesta del Root DNS Server es una lista de IPs que conocen el dominio `.com` a las cuales se les puede consultar por `www.example.com`.

Se elige una IP y se le pregunta por `www.example.com`. Como sucedio con el Root DNS Server, este responde una lista de IPs de servers responsables del dominio `www.example.com` (autoritativos).

Se elige una IP y se le pregunta por `www.example.com`, en este caso el servidor autoritativo responde con la IP correspondiente del nombre.

El DNS Server ahora le responde a tu equipo.

## 12.Diferencia entre módem telefónico y conversor analógico digital.

Cuando se envían datos por un canal de transmisión analógico (una linea telefónica normal) es preciso MODular la señal en origen y DEModularla en el destino. Esto lo hace el MODEM.

Cuando mandamos una señal analógica por un canal de transmisión digital tenemos que CODificarla en origen y DECodificarla en destino. Esto se hace con un CODEC.

## 13.¿Existen sistemas criptográficos "perfectamente seguros" bajo la definición de Shannon? ¿Son utilizados en redes de información?

La respuesta es si: [https://en.wikipedia.org/wiki/One-time\\_pad](https://en.wikipedia.org/wiki/One-time_pad). Si Shannon demostro que one-time pad es perfectamente seguro si se utiliza

para generar la clave un fuente totalmente aleatoria. No son utilizados en redes de informacion o no mucho, ya que requieren de un canal seguro para transmitir la clave.

14. Cuales son los mecanismos propuestos para evitar el problema de conteo a infinito en los protocolos de ruteo basados en algoritmos tipo distance-vector (RIP)?

Split horizon

Split horizon with poisson reverse

15. El mecanismo de establecimiento de una conexión en TCP presenta una vulnerabilidad conocida desde hace decadas. Explique la misma.

Syn Flood - Ataque DoS

Posible defensa: Syn Cookies

16. Que controles de errores se realizan en nivel 2, 3 y 4?

N2: errores de alteracion de bits del medio de transmision.

N3: errores de ruteo (TTL, Unreachable destination, ICMP, dropeo, etc).

N4: mensajes perdidos o fuera de secuencia.

Por control de errores, puede referirse a errores de alteración de bits por ruidos en el medio o errores de pérdida o desorden de paquetes.

Errores de alteración de bits:

Nivel 2: CRC. Nivel 3: Checksum header. Nivel 4: Checksum header.

Errores por pérdida o desorden de paquetes:

Nivel 2: Con stop and wait no se responde el ACK. Con Go Back N,



se retransmite todo desde el último ACK correcto. Con sliding Window NACK selectivo. Se indica cuál llegó mal.

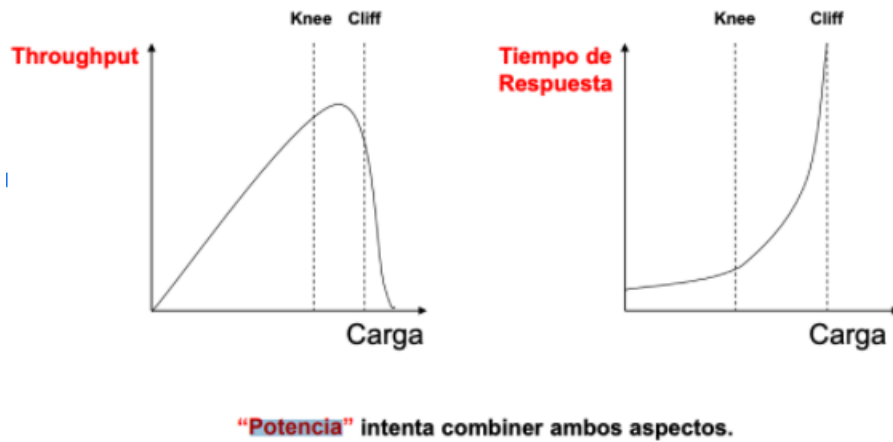
Nivel 3: ICMP. Cuando un paquete llega a TTL 0, se descarta y se envía un msj ICMP. Cuando un paquete se dropea en un router por congestión, también.

Nivel 4: TCP tiene sliding window con ACKS acumulativos. Cuando no llega un ack esperado el emisor retransmite, ya sea por timeout, o por 4 acks duplicados.

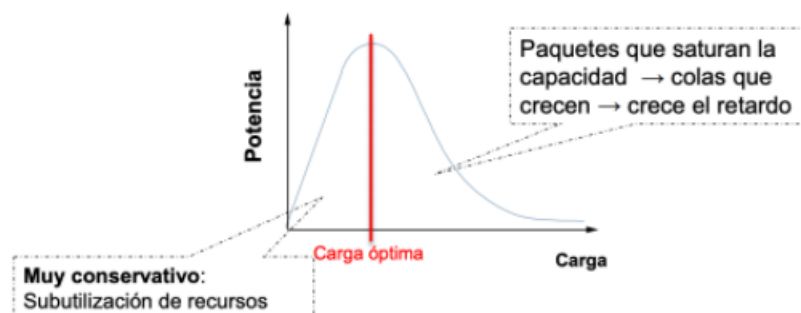
### 17. Como se implementa QoS en ATM.

CLP (Cell Loss Priority) es un campo de celda ATM que indica el nivel de prioridad de la misma, si este bit esta activo cuando la red ATM esta congestionada la celda puede ser descartada. Además, Se puede implementar haciendo control de admisión y reservación de recursos. Al querer establecer el circuito virtual se indican cuántos recursos se van a necesitar, y en caso de poder, se concede y se reservan los recursos. Si no se puede garantizar, se hace control de admisión y se rechaza el nuevo circuito. Esto subutiliza la red, ya que no todos van a estar mandando al mismo tiempo y por ende, tienen reservado más de lo que van a utilizar. Una mejora a esto, es permitir nuevos circuitos, pero con el bit CLP (Cell Loss Priority) del header ATM en 1. Cuando haya que descartar por congestión, los que tienen ese bit en 1, se descartan.

### 18. Graficar throughput y delay en función de carga del sistema. Explicar por qué tienen esa pinta los gráficos.



En estos gráficos podemos observar que a medida que se aumenta la carga de la red se ve un aumento positivo del throughput en detrimento de un aumento del delay. En esta etapa el throughput va aumentando a medida que se explotan más los recursos de la red. Eventualmente se llega al punto en el cual la red se satura por exceso de paquetes circulando, sucede congestión, y se ve afectado el throughput general también (Se empiezan a producir pérdida de paquetes y ocurren TimeOuts). Si tomamos como métrica  $\text{Potencia} = \text{Throughput} / \text{Delay}$  tenemos:



Acá podemos ver cómo hay cierto punto de “Carga óptima” en el cual la red no está saturada de paquetes y se maximiza el uso de sus recursos. Luego, si se le sigue exigiendo más, se deteriora la performance del

sistema por empezar a tener colas más saturadas en los routers y eventualmente decantara en Congestión.

19.Mathis y coautores propusieron en 1997 una expresión para determinar la performance en estado estacionario de TCP Reno:

$BW = MSS * C / (RTT * \sqrt{p})$  con C constante y p probabilidad de error. Describa simplifcadamente la relación que guarda esta expresión con la dinámica de un protocolo de ventana deslizante.. La expresión de performance de ventana deslizante de nivel de enlace es  $MSS/RTT * SWS$  y la expresión de TCP Reno es  $MSS/RTT*(C/\sqrt{p})$  . Se puede tomar  $(C/\sqrt{p})$  como una aproximación del tamaño de la ventana (SWS) ya que el tamaño de la ventana depende de la pérdida de paquetes.

Explique el concepto detrás de la regla empírica  $T < W/C$  en el contexto de un mecanismo de ventana deslizante. Asigne nombres y unidades a cada magnitud. Dibuje un diagrama cualitativo de una evolución temporal típica de la magnitud W en el contexto de un control de congestión en TCP.

Es sobre la fórmula de Mathis. En este caso C es la constante que queda definida en la ecuación de BW y T. La evolución temporal típica de la magnitud W es el gráfico de los dientes de sierra: En función del RTT aumenta constante por Additive Increase y luego se divide a la mitad al suceder un Timeout.

Esto esta en el paper.